Visual Security For Government Credentialing

March 31, 2005

A Document Security Alliance (DSA) Discussion Paper

Purpose:

NIST has issued its final FIPS 201 document covering the minimum requirements for the government's Personal Identity Verification (PIV) card for Federal Employees and Contractors. This FIPS standard specifies the architecture and technical requirements for a common identification standard.

This DSA discussion paper addresses the visual security issues as defined on page 15, paragraph 4.1.2 Tamper Proofing and Resistance, of FIPS 201.

The DSA Concern:

NIST has produced an outstanding standard that defines the MINIMUM requirements for the PIV system. Understandably, the emphasis of FIPS 201 is directed towards the machine readable total system aspects of the government's credentialing program.

The DSA's concern relates to the limited minimum standards defined for visual security protection against counterfeiting, alteration, photo substitution and cannibalization of the card parts. This DSA concern is based on the premise that, even under the government's new smart card credentialing system, the actual ID document will still be used as a visual pass wherever the full card reader and verification system infrastructure is not fully implemented. Accordingly, without sufficient visual security being part of the card's topography, this becomes the weak link in the PIV document system. It is the experience of the DSA that such a visual security breach leads to an ID system compromise very early on in the implementation process and then continues to compromise the security objectives desired.

This issue has been discussed with NIST. The response has been that FIPS 201 defines the minimum requirements; it will be up to the government agencies to add additional security features as part of their Request For Proposals (RFPs/Solicitations).

What Is The DSA?

The Document Security Alliance is a voluntary organization made up of approximately 75 industry members and 20 government agencies that contribute their time to the mission of improving government document security. They do this by combining their broad range of technology knowledge to produce generic guidelines and white papers related to security issues. They function under the lead of the US Secret Service and meet quarterly in the pursuit of solutions that aid and assist government agencies.

The DSA Assumption:

Even though FIPS 201 is based on IC module machine verification, DSA feels strongly that there will continue to be an undefined percentage of manual verifications of the credential for the foreseeable future. This DSA conclusion is based on the experience of other machine readable ID systems and the plain reality associated with the universal authentication process for ID systems. While physical verification may be the exception, it still represents the method by which the ID system will be compromised unless the appropriate visual security features are part of the card system topography. If the reader accepts this premise, then the following information is critical for achieving the ultimate level of protection against counterfeiting, alteration, photo substitution and card document cannibalization. If the reader disagrees with this premise, then it is suggested that a dialogue be instituted between the government agency and the DSA in order to fully inform the decision makers regarding the provision of additional visual security devices. The ultimate decision is that of the government agency, but it needs to be made based on the best information available from those who are most knowledgeable on the subject.

Worldwide Security Trends For ID Systems:

With the introduction and continuing sophistication of desktop color printers and color laser copiers, readily available image editing software packages such as Adobe Photoshop®, the internet and digital cameras, counterfeiting, alteration and photo substitution have become simple processes that the general population can carry out. Accordingly, worldwide security technology experts - including those that are members of the DSA – have emphasized that one visual security feature is no longer sufficient to protect ID documents from such fraudulent actions. Today, layering of security features across all components that make up the ID document is strongly recommended. Driver licenses issued by all jurisdictions in North America will have a minimum of six security features; two of which are overt, two covert, one forensic and one common identifier that will appear in the same position using the same design for all driver licenses issued in North America. These security features will be layered in the various components that constitute the ID document system. Security feature layering produces an extensively more difficult document to counterfeit/alter.

While the FIPS 201 task force believes that the PIV document will be machine verified at all locations very early on in the program, the DSA strongly feels that reality provides a different scenario. The implementation of a government-wide infrastructure to authenticate and read an ID card is an enormous undertaking. Given that the universal system's issuance of new ID cards to large numbers of government employees will take a period of time, secure visual inspection will remain a requirement at least in the interim. The more successful the ID card program, the more widely the card will be accepted, requested and inspected as the *de facto* means of ID. In such a situation ease of secure, visual authentication is essential. We must keep in mind that, while this is a US Federal Government smart card ID, it will be used throughout North America and probably the world as a "right-of-passage" document by airlines any other agencies charged with maintaining security. Indeed, the very Bills that are winding their way through the Halls of Congress refer to the use of government issued picture IDs as a form of acceptable identification. Clearly, these government IDs will not be machine read at non-government locations charged with verifying access to areas subject to potential terrorism. Ideally, selected security features will combine easily verified visual authentication of the card and verification of the card holder's information and identity. These features should be unalterable and serve to confirm other information visible on the card.

Additionally, agencies should include at least one covert feature (requiring a simple magnifier or special light to read) supporting second level verification. Also, forensic features, known only to a select group will support laboratory inspection and criminal investigation. This layering and blending of overt, covert and forensic features provides progressive, hierarchical steps in the visual authentication process and an unequalled level of counterfeit resistance.

Typical criminal attacks on ID documents include the production of "look-alikes" or the altering of genuinely issued documents to another identity, e.g., by photo or image substitution.

Forensic experts strongly advise card and document issuers not to rely on one security feature alone for counterfeit and tamper resistance. They generally favor a "layers on the onion" approach where a combination of features collectively raises the hurdle for criminals seeking to compromise the system.

It is also advisable to consider security devices which include covert features capable of being authenticated either with a simple, inexpensive tool, or by a purpose-built automated device. Such tools can be used in the field or in forensic laboratories to verify suspect documents which may have been the subject of a fraudulent attack.

Successful visual counterfeiting attacks can have enormous cost implications – requiring massive rebadging of high value credentials. Worse yet if the attack goes undetected for a period of time, the result could be a catastrophic security breach. Both possibilities are less likely if the credential incorporates layered security.

FIPS 201 Visual Security Requirement:

On page 15 of the FIPS 201 standards, NIST defines the MINIMUM requirements for visual security in paragraph 4.1.2, Tamper Proofing and Resistance. They call out the use of at least one of the following generic technologies:

- Optical varying structures
- Optical varying inks
- Laser etching and engraving
- Holograms

- Holographic images
- Watermarks

DSA's Recommendations:

It is DSA's strong recommendation that the government agencies call for at least four security features in their RFP/solicitation. These security features should consist of two overt devices one of which is in the card substrate material and one fused to the inside of the overlaminate material. The third security feature would be covert and could be fused to either ID document component. The fourth should be forensic feature for which design and location are only shared with forensic personnel. The combination of these security features will provide the highest level of protection against the fraudulent actions defined in this DSA paper. They can be chosen from the generic categories listed in the FIPS 201 defined above and from the list of over fifty generically described security features listed in the attachment to this document. This attached list has been extracted from a specification used by numerous government agencies. The list also includes whether the security feature is overt, covert, forensic, or a combination. It is important to note that by layering visual security features across the document's components, the credential does not become valid until all these components are combined at the point of issuance thereby adding additional protection from fraudulent activities.

DSA has one other major concern that it wishes to share with the government agencies. The FIPS 201 standard provides the listing of security options as called out above. This provides the government agencies with the opportunity to choose security features that present different appearances and different security functionality when viewed manually in the verification process. This is contrary to the objectives being pursued by the PIV program which is to have the credentialing appear the same across all government agencies. Accordingly, while the card topography will be similar, the security features can vary by agency. Since this is an issue that impacts all agencies and since FIPS 201 is a final specification which will not be changed at this juncture, DSA can only alert all agencies to be aware of the problem and to establish comprehensive training programs for those individuals charged with authenticating credentials received from any of the government agencies.

DSA Point On Durability:

By referencing ISO standards on page 15, FIPS 201 defines the criteria with which the government ID documents must comply. In this regard, DSA wishes to point out the experience of North American driver license programs that comply with these same ISO standards.

Over the last ten years it has been the experience of driver license programs throughout North America that, in order to meet those sections of the ISO standards that relate to durability and long-term performance, the variable imaging (photo, name, etc…) must be overlaminated with a rigid clear plastic. In many applications, this is achieved through a one mil overlaminate. This overlaminate protects the appearance and security features of the ID document for at least five years and typically significantly longer, based on the jurisdictions' driver license longevity requirements. There are over 70 million drivers licenses issued annually in North America by over 60 jurisdictions. Most, if not all, incorporate a one-mil overlaminate, typically on both sides of the card, in order to achieve their durability, performance and security needs.

Also, the card base material should include durable materials such as a combination of PVC and polyester, or polycarbonate. Experience has shown that a pure PVC card will NOT assure the integrity of the card for a minimum of five years. Also, composite cards consisting of a combination of PVC and polyester have proven to be the most compatible with the printer equipment presently being used for the majority of ID document systems.

Conclusion:

The FIPS 201 standard document is the result of an outstanding effort by many knowledgeable individuals, particularly as it applies to the technology framework upon which the standard is based. It is extremely important to recognize that FIPS 201 defines minimum standards and that it is primarily related to the machine readable ID system attributes.

DSA has brought up to the FIPS 201 team its concerns regarding the lack of adequate visual security required for human verification of the credential. We were advised that the standard will not be

changed, but DSA has the option of advising the government agencies of its concerns. The agencies then have the option of increasing these minimum standards in order to achieve a more secure document.

This DSA paper has as its objective, the understanding by all government agencies that at least two overt security features, one covert security feature and one forensic security feature be included in their RFP/solicitations for the PIV system in order to protect the integrity of the government credentialing program. This need not only applies for ID use within the federal government but also for the far broader verification processes that take place outside the government agencies. This additional security can be added with minimal impact to the total cost of the card.

ID Security Device Attachment

Introduction

The security device attachment was developed as a tool to aid in the security design of ID documents and to insure full coverage of common threats to document integrity in North America. The attachment is designed to be inclusive of security devices available for ID documents. The terms used in the attachment are written to the extent possible generically rather than using trademarked names. It is important to point out that this document does not place a rated performance value on any technology listed. Its purpose is to identify the security technology device and then calls out what Threat Levels & Threat Types are addressed by that security device. Some of the security technologies may not be appropriate for the FIPS 201 program; however, it was concluded by the DSA that the total list should be provided so that the reader has a more comprehensive understanding of the range of security devices currently available.

Threat Levels

Level 1 - A Level 1 security device supports first line inspection.

Level 2 – A Level 2 security device supports second line inspection.

Threat Types

Type 1 – Counterfeit/Simulation

Type 2 – Alteration

Type 3 – Photo Substitution

Type 4 – Cannibalization

Printing

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
a. Deliberate Errors/known flaws A feature is purposely made with an intentional mistake known only to the manufacturer or inspection officials.					x			
b. Duplex Patterns A design made up of an interlocking pattern of small irregular shapes, printed in two colors and requiring very close register printing in order to preserve the integrity of the image.	x	x		x	x	x		
c. Fine line background (Guilloche pattern) A pattern of continuously fine lines constructed by using two or more lines in overlapping bands that repeat a lacy, web-like curve.	x	x	x	x	x	x	x	x

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
d. Fine line foreground A pattern of continuously fine lines constructed by using two or more lines overlapping bands that repeat a lacy, web-like curve.	x	x	x	x	x	x	x	x
e. Front to back (see through) register A design printed on both sides of a card that forms an interlocking image when held to a light source.	x							
f. Ghost Image Half tone reproduction of the original image that is typically printed in the same area as, and behind, personal data.		x	x	x	x			x
g. Layered printing (on lamination) Printing separate elements of the secure design on different layers of the laminated card body materials so that no single layer contains all of the security features and the entire products is only apparent after lamination.	x	x		x				
h. Micro optical imaging Text, line art, gray scale images and multi—reflectivity images are engineered into optical WORM media at high resolution (over 12,000 dpi). Difficult to simulate the printing resolution.	x	x			x	x	x	
i. Microprinting / nanoprinting Miniature lettering which is discernible under magnification. Incorporated into fine line backgrounds or placed to appear as bold lines. Continues to decrease in size as technology improves. Difficult to duplicate.					x			x
j. Moiré pattern (anti-scan/VOID pattern) A new pattern formed by the super positioning of two patterns whose periodicities are not identical. Security designs can be developed so that a scanner or copier will only display part of the pattern and/or word VOID or COPY appears instead of the pattern.					x	x	x	x
k. Non standard type fonts Special type that is not available on the commercial market and is reserved for security card use only.	x	x			x	x		
l. Rainbow printing Must demonstrate a controlled exacting color shift subtly in a linear continuous fashion. Accurately designed patterns cannot be easily copied or duplicated via scanning. It is applied using non-commercial method of printing. It is often used with a fine line or medallion pattern in the background of a card.	x							
m. Security code High-resolution color printing systems print a security code within the body of the color printed photo image. The code can be printed in a non-proportional font that can imbed characters on the edge or bottom of the printed picture.					x		x	

Inks

PHYSICAL SECURITY FEATURE	Threat Type	LEVEL 1				LEVEL 2			
		1	2	3	4	1	2	3	4
a. Chemically Reactive Contains a security agent that is sensitive to chemicals, i.e., polar and non-polar solvents and bleach, commonly used to alter documents. The chemical reaction is for the ink to run, stain, and bleed to show evidence of document tampering.			x				x		
b. Infrared fluorescent Forms a visible image when illuminated with light in the infrared / red visible part of the spectrum.						x	x		
c. Infrared drop-out Forms a visible image when illuminated with light in the visible part of the spectrum, but cannot be detected in the infrared region.						x	x		
d. Metallic, pearlescent, and iridescent Inks that fluctuate in brilliance depending on the angle of illumination of the viewing. Difficult to mimic the luster and hard to copy or scan.		x	x	x					
e. Metameric The use of a pair of ink colors that differ in spectral composition but match one another under certain lighting conditions. Under incandescent light that may appear the same, but under colored light they appear as different colors.						x			
f. Phosphorescent Contains a pigment that glows when exposed to a light source of appropriate wavelength. The reactive glow decays after the light source is removed.						x	x		
g. Tagged Contains taggants or compounds that are not naturally occurring and that can be detected using special equipment that reacts to electromagnetic energy identifying the grouping or type.						x			
h. Thermochromatic Ink that exhibits a sharp, reversible color change when exposed to heat, i.e., finger rubbing or hot air.		x				x	x		
i. Ultraviolet fluorescence Invisible inks that emit visible color under exposure to ultraviolet light. Colors can be formulated that are not commercially available, making resistance to counterfeiting higher.						x	x	x	x

Substrate Inclusion

PHYSICAL SECURITY FEATURE	Threat Type	LEVEL 1				LEVEL 2			
		1	2	3	4	1	2	3	4

PHYSICAL SECURITY FEATURE (Threat Type)	LEVEL 1				LEVEL 2			
	1	2	3	4	1	2	3	4
a. Core inclusion The manufacture of card stock with different layers. A colored core material may be placed inside to create a colored edge along the card.	x							
b. Embedded thread, fiber or planchette Small, often fluorescent particles or platelets incorporated into a card material at the time of manufacture that can be seen later under certain lighting conditions. The embedded elements may have magnetic or other machine-readable properties that may be used to enhance the levels of security provided.					x	x		
c. Opacity mark Similar to a watermark, it is a plastic that contains a unique translucent mark.	x							
d. Security bonding The card periphery incorporates a security bonding material that bonds all of the layers together. Tamper evidence is seen if access is attempted to obtain the internal structures of the card.					x	x		x
e. Ultraviolet features Card bodies are made UV dull or possess a controlled response to UV light so they exhibit fluorescence that can be distinguished in color from the "blue" used in commonly available fluorescent materials.					x	x		

Optically Variable Devices (OVD)

PHYSICAL SECURITY FEATURE (Threat Type)	LEVEL 1				LEVEL 2			
	1	2	3	4	1	2	3	4
a.1 Metalized DOVID (Diffractive Image) Opaque metalized DOVID (diffractive optically variable image device). OVD authentication effects cannot be photo copied or digitally recreated. OVDs are holographically mastered or digitally mastered using computer-guided lasers or electron beams.	x	x	x					
a.1.1 De-Metalized OVD (Diffractive Image) A combination of metal and transparency on the same foil or laminate. Hi resolution OVD has selective de-metallization, either transparent or opaque, as defined above.	x	x	x					
a.2. Transparent DOVID Transparent DOVID (diffractive optically variable image device). When incorporated into a ID card design, feature will not interfere with photo or data information. Transparent OVD authentication effects cannot be photo copied or digitally recreated. OVDs are holographically mastered or digitally mastered using computer-guided lasers or electron beams.	x	x	x					
b. Film - Color Shifting OVD	x	x	x					

PHYSICAL SECURITY FEATURE / Threat Type	LEVEL 1				LEVEL 2			
	1	2	3	4	1	2	3	4
Semi-transparent, multilayer light interference film creates noticeable, reflecting color shifts, i.e., clear to blue, magenta to blue, yellow to orange, etc. When incorporated into a ID card design, feature will minimally interfere with photo or data information. OVD color shifting effect cannot be photo copied or digitally recreated.								
c. Ink - Color Shifting OVD Printed opaque, multilayer light interference ink pigment creates noticeable, reflecting color shifts, i.e., gold to green, green to blue, etc. similar to what is seen on many global identification documents including driver licenses, banknotes, passports, and visas. The color shifting and authentication effect cannot be replicated or digitally recreated. Tightly controlled and only available for the most secure document applications.	x	x						
d. Liquid Crystal - Color Shifting OVD Semi-transparent, liquid crystal light interference layers create noticeable, reflecting color shifts, i.e., orange to green. When incorporated into a ID card design, feature will minimally interfere with photo or data information. OVD color shifting effect cannot be photo copied or digitally recreated.	x	x	x					
e. Personalized OVD OVD that is personalized for each card based upon biographical data, portrait, or signature of the cardholder.	x	x	x	x	x	x	x	x
f. Virtual Image OVD Transparent or semi-transparent virtual image appears to float above or sink below the surface of the document, as the viewing angle changes. When incorporated into a ID card design, feature will not interfere with photo or data information. OVD virtual image effect cannot be photo copied or digitally recreated.	x	x	x					

Additional Features

PHYSICAL SECURITY FEATURE / Threat Type	LEVEL 1				LEVEL 2			
	1	2	3	4	1	2	3	4
a. Biometric feature (template) A biometric template of the customer's physical characteristics.					x	x	x	x
b.Covert Device – Readable and Storage Technology Unique individual Near IR or IR invisible data mark, 2-dimenional encrypted bar code, capable of storing independent information or details					x	x	x	x
c. Covert variable pixel manipulation Covert dot matrix images that are converted to visible text with a					x	x	x	x

PHYSICAL SECURITY FEATURE / Threat Type	LEVEL 1				LEVEL 2			
	1	2	3	4	1	2	3	4
special reader or lens.								
d. Digital Seal A method of securing and validating data by electronic means using digital signature technology. The issuing authority "signs" the information contained in the MRT .					x	x		x
e. Embedded Image An image or information that is embedded or encoded within a primary visual image.					x	x	x	x
f. Laminates (security) Transparent layers or films with an integrated security feature(s) are applied to the card with an adhesive or fused by heat. Available in a number of forms, security laminates are designed to be tamper evident and carry other security features to the card.	x	x	x	x				
g. Laser encoded optical image Image and text files are placed to an optical WORM media as a visible diffraction pattern image that is eye-readable under a variety of lighting conditions.	x	x	x					
h. Laser engraving The information cannot be mechanically or chemically removed without surface damage to the card. Can be used for photos, characters, bar codes, OCR, etc.	x	x	x			x		
i. Laser perforation Holes are made with the laser beam of images or objects. The image is visible when held up to a light source. It has a tactile feel with conical holes that are larger at the entrance than exit.	x	x	x	x				
j. Machine readable technology (MRT) Magnetic stripe, smart card, bar codes, OCR, optical WORM media, etc. Verifies the authenticity of the document, the data or the person presenting the card by the use of a reader and comparison of the stored data to other information.					x	x	x	x
k. Magnetic media fingerprinting Tracks unique, random patterns of magnetic media formed as a by-product manufacture of card. The pattern is recorded at the time the card is encoded and this pattern can later be compared to the pattern detected when the card is scanned.					x	x		x
l. Optical media fingerprinting Tracks unique, random patterns of optic media (e.g., fibers) on card. The pattern is recorded at the time the card is encoded and this pattern can later be compared to the pattern detected when the card is scanned.					x	x	x	x
m. Optical watermark Fine line images that are engineered into optical WORM medial with a very high resolution (12,000 dpi). The watermark is overwritten with a laser-encoded optical image, locking together a	x	x			x	x		x

PHYSICAL SECURITY FEATURE / Threat Type	LEVEL 1				LEVEL 2			
	1	2	3	4	1	2	3	4
preformatted document security feature with a laser encoded personalization security feature.								
n. Overlay An ultra-thin film or protective coating that may be applied to the surfaced of a card in place of a security laminate and which may contain optically variable features.	x	x	x	x				
o. Overlapping data Variable data, such as digitized signature, seals or text can be placed over another field such as a photo image. Both fields must be altered if a substitution is to take place making it more difficult.		x	x	x	x	x	x	x
p. Redundant data Display of data in more than one location on the card. A visual inspection may determine if all of the fields match. Usually, the data is displayed in a variety of colors and fonts to further deter alteration.		x						
q. Retroreflective device Optical constructions that reflect light such that covert logos become visible over the entire document when viewed using a focused light source or retroreflective viewer. Level 1 capability is based on a distinctive tactile quality.	x	x	x	x	x	x	x	x
r. Security threads Metal or plastic, these threads are seen on currency. With special metallized film, demetallized text is invisible in reflected light and therefore is difficult to copy. When viewed in transmitted light, the opaque aluminum letters are clearly visible.	x	x	x		x	x	x	x
s. Thin film interference filters Multiple layer structures that produced color effects by interference.					x			
t. Tactile feature A feature which is apparent to touch or feel without requiring a special instrument. This could include texture, flexibility, or weight of the document and/or a feature incorporated in the card structure or card components.	x	x						